REMARKS

Claims 1 – 12 are now pending in the application. Applicant respectfully requests that the Examiner reconsider and withdraw the rejection(s) in view of the following remarks.

REJECTION UNDER 35 U.S.C. § 103

The Examiner rejected claims 1 – 12 under 35 U.S.C. § 103(a) as being unpatentable over Applicant's admitted prior art (AAPA) and Caputo et al. (U.S. 5,778,071) in view of Hayosh (U.S. 6,212,504) for the same reasons given in the prior Official Action. Applicant respectfully traverses this rejection.

The invention pertains to the way in which a data transaction terminal recognizes a data entry prompt from a remote device as a "secure prompt" in order to determine whether it is appropriate to transmit data entered into it in response to the data entry prompt as "clear text" data. More particularly, it pertains to the ability to recognize a data entry prompt as a "secure prompt" when the data entry prompt is not identical to the prompts stored in a secure prompt table. "Clear text" data, as defined in the Application, is data that is transmitted in a standard format, such as ASCII, without securing using techniques such as encryption. [Application, Par. 4]

In order to prevent the interception of sensitive information, the PED Spec. imposes certain requirements on when data input into the data transaction terminal can be transmitted as "clear text" data in response to a data entry prompt. Of pertinence here, the PED Spec. requires that data input into the data transaction terminal can be transmitted as "clear text" data only if it was input in response to a data entry prompt, calling for the entry of non-sensitive data. The Application uses the term "secure prompt" to refer to a data entry prompt that calls for the entry of

non-sensitive data. In this regard, the Application expressly defines "secure prompt" "as a prompt that prompts for the entry of non-sensitive data, such as odometer readings." [Application, Par. 6]

Claims 1, 2, 4, 6, 8, 10 and 12 are the independent claims. Turning first to claim 1, claim 1 is directed to a security method for transmission to a remote device of data input into a transaction terminal as clear text data. Claim 1 recites, in pertinent part:

> "(b) determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:
>
> (i) the data entry prompt matching at least one of the prompts in the secure prompt table,
>
> (ii) the data entry prompt matching only a portion of any of the secure prompts in the secure prompts table, and
>
> (iii) any of the prompts in the secure prompt table matching only a portion of the data entry prompt."

The Examiner concedes that the AAPA does not disclose these limitations. But the Examiner takes the position that Caputo et al. discloses "a digital algorithm (algorithm or plain text data) that includes a private/public keys [sic] or portion of the secure prompts." The Examiner then asserts that it would have been obvious to modify the teaching of AAPA with Caputo et al. because this would prevent unauthorized access to the system using the encryption algorithm.

Applicant's invention is not directed to preventing unauthorized access to the data transaction terminal. Applicant's invention is directed to the way in which a data transaction terminal recognizes a data entry prompt as a "secure prompt" to determine when it is appropriate to transmit data input into the data transaction terminal in response to a data entry prompt as "clear text" data.

Applicant submits that the Examiner is construing the term "secure prompt" in a manner inconsistent with its express definition in the Application and only by doing so can find that the private/public keys of Caputo et al. are readable as "secure prompts. The Examiner does not explain why private/public keys are readable as "secure prompts." Applicant assumes that the Examiner's position is that since private/public keys deal with transmitting data in a secure fashion, they are "secure prompts." This, however, is not consistent with the definition of "secure prompts" in the Application. As discussed above, the Application defines "secure prompt" as a data entry prompt that prompts for the entry of non-sensitive data. Caputo et al. simply does address the use of data entry prompts, let alone data entry prompts sent to a data transaction terminal to prompt for the entry of data. Caputo et al. thus does not need to deal with determining whether a data entry prompt is a "secure prompt" or not.

Caputo et al., as discussed in Applicant's response to the prior Official Action, is directed to a portable security device that can be carried by an individual and connected to telephone circuits to both authenticate the individual and encrypt data communications. [Caputo et al., Abstract] With regard to the sections of Caputo et al. cited by the Examiner, the first section, col. 10, lines 51 – 67, simply discloses that Caputo's et al. data is encrypted before it is transmitted. The second section of Caputo et al. cited by the Examiner deals with the sender of the encrypted data authenticating it and the receiver verifying it, as can be seen by the discussion in Caputo et al. that introduces the second section cited by the Examiner. [See, Caputo et al., col. 12, lines 14 – 17]. But a sender authenticating encrypted data and the receiver verifying it does not involve a method for transmitting data in clear text form in response to a secure prompt and does not involve determining when a data entry prompt is a secure prompt. The third section of Caputo et al. cited by the Examiner deals with device and user

authentication, i.e., digital signatures, as can be seen from the section of Caputo et al. introducing the third section cited by the Examiner. [See, Caputo et al., col. 14, lines 10 - 14]. This again does not deal with transmitting data in clear text form in response to a secure prompt and does not involve determining when a data entry prompt is a secure prompt.

Moreover, using public/private keys of Caputo et al. as "secure prompts," as the Examiner proposes, teaches away from the claimed invention. Public/private keys are inputs to algorithms that use the private key to encrypt data and the public key to decrypt the data. The exact keys must be used or the data when decrypted will be unrecognizable. As is commonly understood by those familiar with public/private keys, the exact keys must be used or the algorithms will not return valid results. Assuming that public/private keys are used as prompts, doing so would thus require that the exact keys be used. Using only part of a private key as a data entry prompt would result in a data entry prompt that would be unrecognizable when the public key is used to interpret it, and vice-versa. This is the opposite of what claim 1 requiers. As discussed above, claim 1 includes limitations directed to recognizing a data entry prompt as a secure prompt when there is not exact identity between the data entry prompt and the prompts in the secure prompt table. More specifically, claim 1 includes limitations directed to recognizing a data entry prompt as a secure prompt when the data entry prompt matches only a portion of any of the secure prompts in the secure prompt table and when any of the prompts in the secure prompt table match only a portion of the data entry prompt. The Examiner has failed to show where Caputo et al. discloses determining that a data entry prompt is a secure prompt when only a portion of the data entry prompt matches any of the secure prompts in the secure prompt table or any of the prompts in the secure prompt table match only a portion of the data entry prompt.

Hayosh also fails to disclose the use of secure prompts, and thus cannot disclose determining that a data entry prompt is a secure prompt upon the occurrence of any of the conditions recited in claim 1, and the Examiner does not cite it as doing so. Rather, the Examiner cites Hayosh as disclosing a digital signature with clear text data. Applicant's invention is not directed to using a digital signature with clear text data, but determining whether a data entry prompt is a secure prompt and transmitting data in clear text form only upon determining that the data entry prompt is a secure prompt. Applicant submits that the combination of Hayosh with Caputo et al. and the AAPA thus fails to disclose or suggest Applicant's invention as claimed in claim 1.

For many of the same reasons expressed above, and as discussed in Applicant's response to the prior Official Action, Applicant submits that claims 2, 4, 6, 8, 10 and 12 are allowable. For convenience, Applicant includes the arguments in the response to the prior Official Action below.

Claim 2 recites, in pertinent part:

> "(b) determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:
>
> (i) the data entry prompt matching any prompt in the secure prompt table, and
>
> (ii) the data entry prompt matching only a portion of any prompt in the secure prompt table."

Again, the Examiner admitted that the AAPA does not disclose these limitations. Neither does Caputo et al. or Hayosh. As discussed, Caputo et al. does not disclose or discuss determining whether a data entry prompt is a secure prompt, and thus cannot disclose or suggest doing so based upon any of the conditions recited in claim 4. Similarly, Hayosh also does not disclose or discuss determining whether a data entry

prompt is a secure prompt. Applicant submits that claim 2 is thus allowable over the combination of the AAPA, Caputo et al. and Hayosh.

Claim 4 recites, in pertinent part:

"(b) determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i) the data entry prompt matching any prompt in the secure prompt table, and

(ii) any prompt in the secure prompt table matching only a portion of the data entry prompt."

Again, the Examiner admitted that the AAPA does not disclose these limitations. Neither does Caputo et al. or Hayosh. As discussed, Caputo et al. does not disclose or discuss determining whether a data entry prompt is a secure prompt, and thus cannot disclose or suggest doing so based upon any of the conditions recited in claim 4. Hayosh also does not disclose or discuss determining whether a data entry prompt is a secure prompt. Applicant submits that claim 4 is thus allowable over the combination of the AAPA, Caputo et al. and Hayosh.

The remaining independent claims, claims 6, 8, 10 and 12, contain limitations comparable to the limitations discussed above with respect to one or more of claims 1, 2 and 4. Applicant submits that claims 6, 8, 10 and 12 are thus allowable over the combination of the AAPA and Caputo et al..

The dependent claims, claims 3, 5, 7, 9 and 11 depend from respective ones of the independent claims and are allowable for at least that reason.

CONCLUSION

Applicant submits that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw all presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office Action, and as such, the present application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (248) 641-1600.

Respectfully submitted,

Dated: Dec. 15, 2004

By: R. A. Fuller III
Roland A. Fuller III, Reg. No. 31,160

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600
RAF/akb